CHAPTER

# 10

# IMPLEMENTING GROUP POLICY

**After completing this chapter, you will be able to:**

- Understand Group Policy concepts
- Plan an effective Group Policy design
- Implement Group Policy

Windows 2000 dramatically improves the ability of systems administrators to exert control of the user environment, compared to Windows NT 4. With Group Policy, an administrator can define a large number of detailed settings that are applied throughout the organization. In fact, in Windows 2000, Group Policy is now the primary means of applying, to users and computers, changes that are enforced across an organization.

In this chapter, we will look at the basics of implementing and administering Group Policy. In subsequent chapters, we will expand our discussion to include managing user environments and deploying software with Group Policy.

# Understanding Group Policy Concepts

Group Policy is a power tool for network administrators to control any number of environment settings across an enterprise. Implementing Group Policy can greatly reduce the administrative overhead for a network, reducing total cost of ownership (TCO) and increasing return on investment (ROI) for Windows 2000. Although TCO and ROI issues might sound more like business terms than technological terms, increasingly MIS departments are being expected to function as business units rather than just as cost centers. The enlightened information systems professional learns to understand how to apply technology from a business perspective, and how to maximize a corporation's investment in technology systems.

Before we can delve into implementing Group Policy, however, we must examine some basic concepts such as:

- Windows 2000 Group Policy versus Windows NT 4 system policies
- Group Policy Objects (GPO)
- The Group Policy Microsoft Management Console (MMC) snap-in
- Group Policy namespace
- Startup, shutdown, logon, and logoff
- Active Directory structure and Group Policy
- Group Policy inheritance
- Group Policy processing

## Windows 2000 Group Policy versus Windows NT 4 System Policies

With Windows NT 4, Microsoft introduced system policies. These policies are edited through the poledit.exe utility; they give the administrator the ability to define user environment settings stored in the Registry. System policies allow specific configuration settings to be enforced on any Windows NT 4 workstation or server in a domain.

With Windows 2000, Group Policy provides all of the functionality of system policies and more. You use the Group Policy MMC snap-in rather than poledit.exe, although poledit still exists for backward compatibility. It is important to note, however, that poledit.exe has been updated for Windows 2000; the format of the POL files created in Windows 2000 is different from the format of the files created in Windows 9*x* and NT 4. Policies created with the Windows 9*x* or NT 4 policy editor cannot be applied to Windows 2000 systems—but policies created in Windows 2000 with poledit.exe *can* be applied to Windows 9*x* and Windows NT 4 clients.

For Windows 2000 workstations and servers, however, Group Policy all but replaces system policies. Group Policy provides a more flexible means to apply and enforce configuration settings; even more important, it allows for a much more granular approach. Whereas system policies can be applied only to domains, Group Policy can be applied to sites, domains, and Organizational Units (OUs). The following sections compare and contrast NT and Windows 9*x* system policies with Windows 2000 Group Policy.

## Windows NT 4 and Windows 9x System Policies

System policies have the following features:

- They are applied only to domains.
- They are limited to Registry-based settings an administrator configures.
- They are not written to a secure location of the Registry. Hence, any user with the ability to edit the Registry can disable the policy settings.
- They often last beyond their useful life spans. System policies remain in effect until another policy explicitly reverses an existing policy or a user edits the Registry to remove a policy.
- They can be applied through NT domain security groups.

## Windows 2000 Group Policy

Group policies have the following features:

- They can be applied to sites, domains, or OUs.
- They can be applied through domain security groups, and can apply to all or some of the computers and users in a site, domain, or OU.
- They are written to a secure section of the Registry, which prevents users from being able to remove a policy through the regedit.exe or regedit32.exe utility.
- They are removed and rewritten whenever a policy change takes place. Administrators can set the length of time between policy refreshes, ensuring that only the current policies are in place.
- They provide a more granular level of administrative control over a user's environment.

In addition, Windows 2000 Group Policy provides features not available through system policies, such as additional system startup/shutdown control and folder redirection. These features will be covered later in the chapter.

## Group Policy Benefits

When properly implemented, Group Policy can reduce the TCO for a Windows 2000 network. One of the more common causes of lost productivity among corporate users is system downtime due to user-induced errors. These errors can result when users modify or delete critical system files, or when they waste time playing with screen savers, games, wallpaper, and other operating system features. Through Group Policy, you can create a managed user environment that provides a consistent interface for users of certain experience levels.

Group Policy can also be used to enhance the end user's computing experience by providing customized environments to meet the user's work requirements. Such customization might include putting specialized application icons on the desktop or Start menu, or redirecting the My Documents folder to a network drive so the user's files are available no matter what computer they log on to. In addition, an administrator can execute such tasks as startup, logon, logoff, or shutdown to meet the user's needs. In this light, Group Policy can create a positive working environment for users.

### Managing User Expectations

From the end user's perspective, system policies/group policies are often viewed negatively. Many users see managed desktops as a sign of distrust from management, or they feel they are not being allowed any individuality. This viewpoint is an important aspect of desktop management to consider, especially if Group Policy will be applied to desktop systems that have been open to user configuration in the past. Although few would argue that the computers belong to the company and therefore they can be managed in any way that will best suit the company, the psychology of the situation must be handled delicately. If it is not, any efficiency gains from desktop management may be offset by lost productivity from declining employee morale. Restrictive services such as policies, e-mail mailbox limits, and disk quotas are better implemented from the beginning rather than in midstream, to minimize the impact on morale. But if they must be implemented after the network is initially set up, be sure to consider the employee mindset and keep communication channels open between users and management.

## Group Policy Objects

The collection of Group Policy settings are stored in what are known as Group Policy Objects (GPOs). There are two types of GPO: local and non-local. Local GPOs are stored on each Windows 2000 computer, whereas non-local GPOs are stored at the domain level within Active Directory.

### Local GPOs

A local GPO exists on each Windows 2000 computer, and by default only the settings under the Security node of Group Policy apply. Local GPOs are stored in the \winnt\system32\GroupPolicy folder. Through discretionary access control lists, the following permissions are set:

- *Administrators*—Full Control
- *Operating System*—Full Control
- *Authenticated Users*—Read

The easiest way to prevent local GPOs from applying to a computer is to remove Read permissions from the Local Administrators group. Even if Apply Group Policy is set to Allow, this setting cannot be applied if the GPO cannot be read.

## Non-Local GPOs

Non-local GPOs are stored at the domain level within Active Directory. As such, they apply at the site, domain, and OU level. Two locations are used to store non-local GPOs: a Group Policy container and a Group Policy template. A globally unique identifier (GUID) is used in naming the GPOs to keep the two locations synchronized.

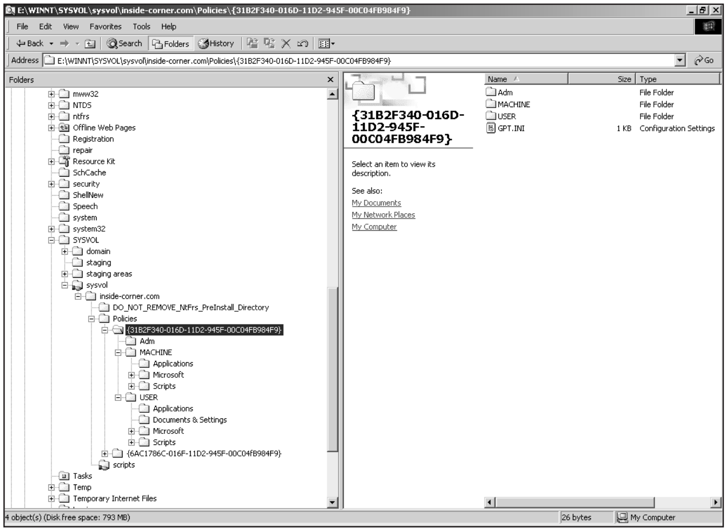
A Group Policy container is an Active Directory storage area for GPO settings for both computer and user Group Policy information. The Group Policy container includes the following information:

- Version information, ensuring that the information in the Group Policy container is synchronized with the Group Policy template information
- Status information, indicating whether the GPO is enabled or disabled
- The list of extensions that have settings in the GPO
- The policy settings defined by the extensions

An example of an extension would be the Software Installation snap-in. The Group Policy container stores information used by the snap-in to describe the status of software available for installation. A server-based repository contains the data for all applications, interfaces, and Application Programming Interfaces (APIs) used in application publishing and assigning.

In addition to the Group Policy container, Active Directory stores information in a Group Policy template, which is contained in a folder structure in the System Volume (SYSVOL) folder of domain controllers. Figure 10-1 shows this directory structure, located under \winnt\SYSVOL\sysvol\*domain_name*\Policies.

When a GPO is created, the Group Policy template is created with the folder structure shown in Figure 10-1. The folder name given to the Group Policy template is the GUID of the GPO. In our example, the GUID and folder name is {31B2F340-016D-11D2-945F-00C04FB984F9}. Table 10-1 shows a breakdown of the Group Policy template subfolders.



E:\WINNT\SYSVOL\sysvol\inside-corner.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}

Address E:\WINNT\SYSVOL\sysvol\inside-corner.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}

{31B2F340-016D-11D2-945F-00C04FB984F9}

Select an item to view its description.

See also:
My Documents
My Network Places
My Computer

| Name | Size | Type |
|---|---|---|
| Adm | | File Folder |
| MACHINE | | File Folder |
| USER | | File Folder |
| GPT.INI | 1 KB | Configuration Settings |

4 object(s) (Disk free space: 793 MB)

26 bytes

My Computer

**Figure 10-1** Group Policy template information is stored under the SYSVOL folder structure

**Table 10-1** The structure of Group Policy template subfolders

| Subfolder | Contents |
|---|---|
| \ADM | The ADM files (administrative templates) for a Group Policy template. The ADM file consists of a hierarchy of categories and subcategories that together define how the options are displayed through Group Policy. |
| \Machine | A Registry.pol file that includes the Registry settings to be applied to computers. When the computer boots up, the Registry.pol file is applied to the HKEY_LOCAL_MACHINE portion of the Registry. |
| \Machine\Applications | AAS files (application assignment scripts) used by Windows Installer. These files contain instructions associated with the assignment or publication of a package. |
| \Machine\Microsoft\ Windows NT\SecEdit | The GptTmpl.inf Security Editor file. |
| \Machine\Scripts\Startup | Scripts that apply to the computer during startup. |
| \Machine\Scripts\Shutdown | Scripts that apply to the computer during shutdown. |
| \User | Includes a Registry.pol file that applies to users as they log on. The Registry.pol file is applied to the HKEY_CURRENT_USER portion of the Registry. |
| \User\Applications | AAS files used by the Windows Installer. |
| \User\Documents & Settings | Files to deploy to all desktops for all users utilizing this Group Policy template. |

**Table 10-1** The structure of Group Policy template subfolders (continued)

| Subfolder | Contents |
|---|---|
| \User\Microsoft\IEAK | Information about settings the Internet Explorer Administrator Kit uses for deploying IE settings to the desktop. |
| \User\Microsoft\RemoteInstall | The oscfilter.ini file, which includes policies about Remote Installation Services (RIS). |
| \User\Scripts\Logoff | Scripts that apply to the user during logoff. |
| \User\Scripts\Logon | Scripts that apply to the user during logon. |

In the contents pane of Figure 10-1, you will notice a file called GPT.INI. The root folder of each Group Policy template contains this file, which includes information about whether the local GPO is enabled or disabled, the version number, and which client-side extensions of Group Policy contain user or computer data in the GPO.

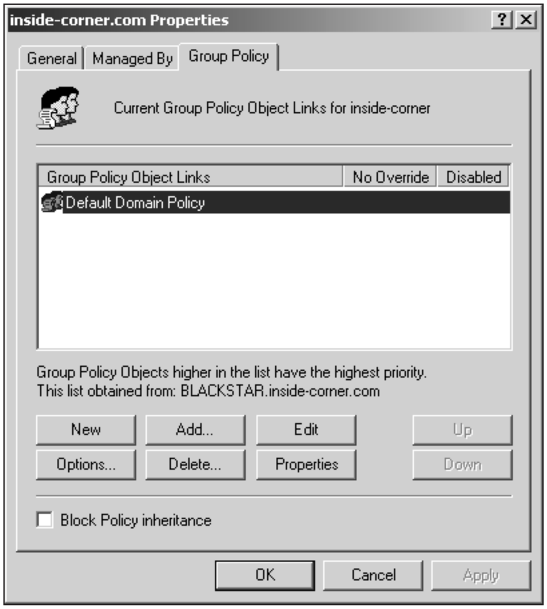
How does Windows 2000 determine what to store in a Group Policy container versus a Group Policy template? Data that is small in size and that changes infrequently is stored in Group Policy containers, whereas data that is either large in size or that changes frequently is stored in Group Policy templates.

## The Group Policy MMC Snap-in

In order to edit Group Policy Objects, you will need to open the Group Policy Editor. By default, there is no single Group Policy administrative tool. The Group Policy Editor can be invoked at a number of different levels depending on your needs. For example, to edit Group Policy settings for a site, launch the Active Directory Sites and Services management console. From there, right-click on the site you want and choose Edit; then, click on the Group Policy tab and click on Edit. Doing so will start a new MMC console, with the Group Policy ready to edit site settings.

Typically, you will edit GPOs at the domain level rather than the site level; you do so through Active Directory Users and Computers. Right-click on the domain and choose Properties to bring up a window similar to that shown in Figure 10-2. Select Default Domain Policy and click on Edit.

When you click on Edit, you will see a console similar to that shown in Figure 10-3. You will use this Group Policy console most of the time.



inside-corner.com Properties

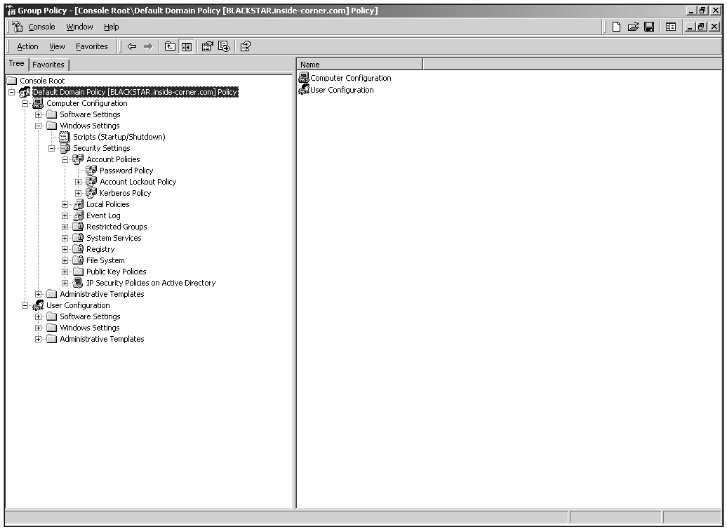
Current Group Policy Object Links for inside-corner

| Group Policy Object Links | No Override | Disabled |
|---|---|---|
| Default Domain Policy | | |

Group Policy Objects higher in the list have the highest priority.
This list obtained from: BLACKSTAR.inside-corner.com

□ Block Policy inheritance

**Figure 10-2** The Active Directory Users and Computers utility can be used to invoke the Group Policy Editor at the domain level



Group Policy - [Console Root\Default Domain Policy [BLACKSTAR.inside-corner.com] Policy]

```
Console Root
  Default Domain Policy [BLACKSTAR.inside-corner.com] Policy
    Computer Configuration
      Software Settings
      Windows Settings
        Scripts (Startup/Shutdown)
        Security Settings
          Account Policies
            Password Policy
            Account Lockout Policy
            Kerberos Policy
          Local Policies
          Event Log
          Restricted Groups
          System Services
          Registry
          File System
          Public Key Policies
          IP Security Policies on Active Directory
      Administrative Templates
    User Configuration
      Software Settings
      Windows Settings
      Administrative Templates
```

| Name |
|---|
| Computer Configuration |
| User Configuration |

**Figure 10-3** The Group Policy MMC snap-in allows you to configure GPOs

You also have the option of creating a custom MMC console with the Group Policy focus you will use most often. By doing so, you can save yourself the time of going through another tool in order to get to Group Policy.

## Group Policy Namespace

The Group Policy snap-in displays the root node as the name of the GPO and the domain in which it is stored. In our earlier example, the node is written as

```
Default Domain Policy [BLACKSTAR.inside-corner.com] Policy
```

The next level of the namespace has the Computer Configuration and User Configuration nodes. Each of those nodes contains the following subnodes:

- Software Settings
- Windows Settings
- Administrative Templates

Let's look at the Computer Configuration and User Configuration nodes and their subnodes in more detail.

### Computer Configuration

The Computer Configuration folders contain all computer-related policy settings that you can use to customize the user's environment at the computer level. These settings can include such things as operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, and application settings. Policies assigned to computers apply to every user who logs on to the computer.

### User Configuration

The User Configuration folders contain all policy settings that you can use to customize the user's environment at the user level. These settings can include such things as desktop appearance, application settings, logon and logoff scripts, assigned and published applications, and folder redirection settings. Policies assigned at the user level apply only to the specific user when he or she logs on to a computer. In general, computer policies will override user policies.

### Software Settings

The Software Settings node is a place for independent software vendors to add further extensions to Group Policy. Initially, only a single Software Installation node will appear under Software Settings—this extension is included with Windows 2000.

### Windows Settings

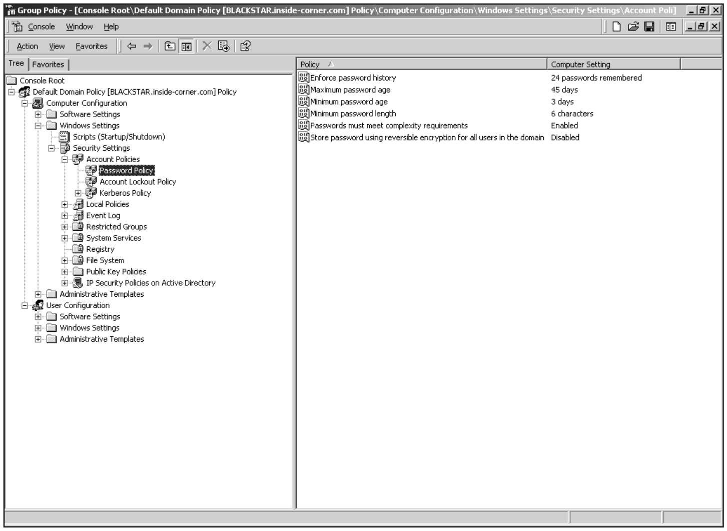
The Windows Settings node contains extensions provided by Microsoft and included with Windows 2000. These extensions include Scripts (startup/shutdown for Computer Configuration, logon/logoff for User Configuration) and Security Settings that apply to both computers and users, and Internet Explorer maintenance that applies specifically to users.

In addition, folder redirection settings are configured under Windows Settings for the User Configuration container, as are Remote Installation Services (RIS) if RIS is installed.

Many administrators find themselves most often in the Security Settings area of Group Policy. This area in Computer Configuration is extensive, covering three core areas:

- Password Policy
- Account Lockout Policy
- Kerberos Policy

The Password Policy settings, shown in Figure 10-4, contain many of the settings you may remember from the Windows NT 4 Account Policies utility.



| Policy | Computer Setting |
|---|---|
| Enforce password history | 24 passwords remembered |
| Maximum password age | 45 days |
| Minimum password age | 3 days |
| Minimum password length | 6 characters |
| Passwords must meet complexity requirements | Enabled |
| Store password using reversible encryption for all users in the domain | Disabled |

**Figure 10-4** You can configure policy settings that affect password requirements

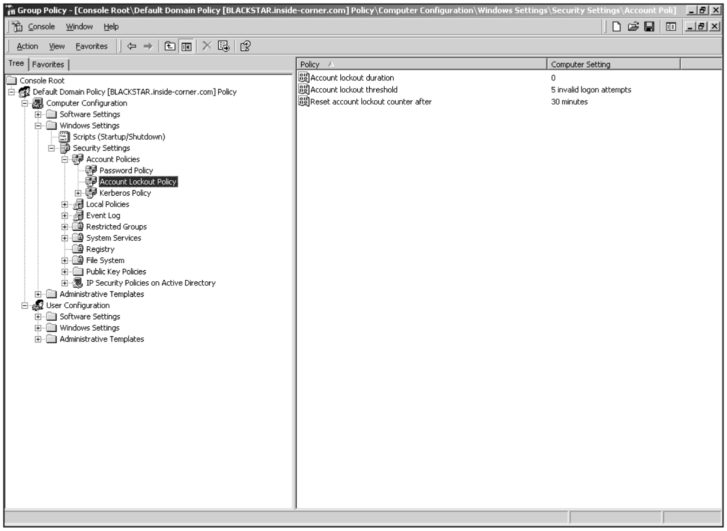
In NT 4, these settings are configured by opening the Policies menu and choosing Account from the User Manager For Domains administrative tool. Administrators of NT 4 systems will notice two new additions in Windows 2000:

- Passwords must meet complexity requirements
- Passwords are stored using reversible encryption for all users in the domain

The first of those options is a great new feature for administrators who struggle with users who undermine password policies by repeatedly choosing a simple password whenever they are required to create a new one. Windows 2000 can now force a password to contain alphanumeric or other characters in addition to remembering a password history and requiring passwords to be a certain length.

From a Group Policy perspective, you as the administrator can employ password policies that apply either to your entire enterprise or locally on a machine-by-machine basis. For example, you may have a few computers in a sensitive area that need more stringent password policies than ordinary domain users require.

Account lockout policies, shown in Figure 10-5, are the same as in NT 4.You can choose how many bad passwords a user can enter in a certain time frame before the account is locked—for example, you might allow three bad passwords in 30 minutes before locking the account. In addition to these settings, you can set the length of time the account remains locked out.The default lockout setting is 30 minutes, at which time the account reverts to its normal state. For better security, we recommend setting the lockout duration to zero, which requires a locked account to be manually unlocked by an administrator. Not only will a potential intruder be unable to pick on a single account unnoticed, but this setting ensures that an administrator is aware of any instances where multiple bad passwords are entered for a user account in a short period of time. Even if such an occurrence is not a sign of malicious activity, it could indicate either a user training issue or a system problem that needs to be addressed.



Group Policy - [Console Root\Default Domain Policy [BLACKSTAR.inside-corner.com] Policy\Computer Configuration\Windows Settings\Security Settings\Account Poli]

| Policy | Computer Setting |
|---|---|
| Account lockout duration | 0 |
| Account lockout threshold | 5 invalid logon attempts |
| Reset account lockout counter after | 30 minutes |

```
Console Root
Default Domain Policy [BLACKSTAR.inside-corner.com] Policy
  Computer Configuration
    Software Settings
    Windows Settings
      Scripts (Startup/Shutdown)
      Security Settings
        Account Policies
          Password Policy
          Account Lockout Policy
          Kerberos Policy
        Local Policies
        Event Log
        Restricted Groups
        System Services
        Registry
        File System
        Public Key Policies
        IP Security Policies on Active Directory
    Administrative Templates
  User Configuration
    Software Settings
    Windows Settings
    Administrative Templates
```

**Figure 10-5** Account lockout policies are much the same in Windows 2000 as they were in Windows NT 4

Windows 2000 uses the Kerberos security protocol.You can use Group Policy to configure the various Kerberos security and ticketing policies that apply to a Windows 2000 domain.

## Administrative Templates

As in Windows NT 4, administrative templates have an .adm extension in Windows 2000. Administrative templates provide a source for Group Policy to generate the policy settings that you can configure. These files provide information about the Registry settings to be modified when an administrator makes a change, the specific settings that correspond to the GPO entry, and (in some cases) a default value if such a value is automatically assigned when a setting is enabled.

Administrative templates created with the NT 4 System Policy Editor can be read and changed with the Windows 2000 System Policy Editor, because Windows 2000 uses a superset of the language supported by NT 4. Because the languages are not the same, however, administrative templates created in Windows 2000 cannot be read by the NT 4 System Policy Editor.

In the Computer Configuration and User Configuration containers, administrative templates are provided with Windows 2000 for the categories and subcategories shown in Table 10-2.

**Table 10-2** The Group Policy categories and subcategories available for computers and users in Windows 2000

| Container | Category | Subcategory | Subcategory |
|---|---|---|---|
| Computer Configuration | Windows Components | Netmeeting | |
| Computer Configuration | Windows Components | Internet Explorer | |
| Computer Configuration | Windows Components | Task Scheduler | |
| Computer Configuration | Windows Components | Windows Installer | |
| Computer Configuration | System | | |
| Computer Configuration | System | Logon | |
| Computer Configuration | System | Disk Quotas | |
| Computer Configuration | System | DNS Clients | |
| Computer Configuration | System | Group Policy | |
| Computer Configuration | System | Windows File Protection | |
| Computer Configuration | Network | Offline Files | |
| Computer Configuration | Network Connections | Network and Dial-up | |
| Computer Configuration | Printers | | |
| User Configuration | Windows Components | Netmeeting | |
| User Configuration | Windows Components | Netmeeting | Application Sharing |
| User Configuration | Windows Components | Netmeeting | Audio & Video |
| User Configuration | Windows Components | Netmeeting | Options Page |
| User Configuration | Windows Components | Internet Explorer | |
| User Configuration | Windows Components | Internet Explorer | Internet Control Panel |

**Table 10-2** The Group Policy categories and subcategories available for computers and users in Windows 2000 (continued)

| Container | Category | Subcategory | Subcategory |
|---|---|---|---|
| User Configuration | Windows Components | Internet Explorer | Offline Pages |
| User Configuration | Windows Components | Internet Explorer | Browser Pages |
| User Configuration | Windows Components | Internet Explorer | Toolbars |
| User Configuration | Windows Components | Internet Explorer | Persistent Behaviors |
| User Configuration | Windows Components | Internet Explorer | Administrator Approved Controls |
| User Configuration | Windows Components | Windows Explorer | |
| User Configuration | Windows Components | Windows Explorer | Common Open File Dialog |
| User Configuration | Windows Components | Microsoft Management Console | |
| User Configuration | Windows Components | Task Scheduler | |
| User Configuration | Windows Components | Windows Installer | |
| User Configuration | Start Menu & Taskbar | | |
| User Configuration | Desktop | | |
| User Configuration | Desktop | Active Directory | |
| User Configuration | Desktop | Active Desktop | |
| User Configuration | Control Panel | | |
| User Configuration | Control Panel | Add/Remove Programs | |
| User Configuration | Control Panel | Display | |
| User Configuration | Control Panel | Printers | |
| User Configuration | Control Panel | Regional Options | |
| User Configuration | Network | Offline Files | |
| User Configuration | Network Connections | Network and Dial-up | |
| User Configuration | System | | |
| User Configuration | System | Logon/Logoff | |
| User Configuration | System | Group Policy | |

Some overlap exists among items that can be configured at both a computer level and a user level, such as certain Windows components, because policies can apply to a computer as a whole or only to certain users of a computer, depending on specific needs. In many cases, there appears to be overlap; however, different sets of policy settings are available depending on whether the configuration is set at the computer or user level. For example, the policy settings under the System root in Computer Configuration and User

Configuration are completely different, because different types of system policies apply to computers than apply to users. In this case, the apparent overlap is *not* an example of the same policies just applied at a different level.

## Startup, Shutdown, Logon, and Logoff

Group Policy can be used to affect the user or computer environment in different ways at different times. Computer policies can be applied at both system startup and shutdown, whereas user policies can be applied at logon and logoff. The combination of the four events can be used to create complex policy configurations for Windows 2000 users. For example, a common script might be run on the computer at startup to affect certain settings that should apply to anyone who uses the computer. User-specific scripts can be run when a user actually logs on to the computer. When a user logs off, you can designate a script to run that performs certain actions such as disconnecting any mapped network drives. In addition, a computer can execute a shutdown script to perform any required actions before it is turned off.

The ability to run scripts at any of these four times offers much more flexibility over Windows NT 4, which allows only for logon scripts. This flexibility gives the Windows 2000 administrator increased control over the user and computer environment.

## Active Directory Structure and Group Policy

As we touched on earlier, there are two types of GPO: local and non-local. GPOs are the basic units of Group Policy, and they can be linked or filtered. Because they are the basic units, only a GPO in its entirety may be linked to another target. That is, you cannot link only a subset of a GPO. The effects of GPOs are actually applied through links, as they are linked to sites, domains, or OUs. If no link exists between a GPO and any other target, then the policy settings will not have any effect.

The exception to linking is that GPOs cannot be linked to generic Active Directory containers, such as the Users container in Active Directory Users and Computers. They receive domain-linked Group Policy through inheritance, however. Inheritance is discussed later in this chapter.

The structure of Group Policy in Active Directory is as follows:

- GPOs linked to a site apply to all domains within the site.
- GPOs applied to a domain apply to all users and computers within the domain, and through inheritance apply to all users and computers in OUs further down the domain structure.
- GPOs applied at the OU level apply to all users and computers within the OU, and through inheritance apply to all users and computers included within OUs that are contained within the OU that is linked to the GPO.
- Local policies are applied first, followed by non-local policies.

- Non-local policies are applied in the following order: site level, domain level, and then OU level, beginning at the highest OU level within the Active Directory tree and ending with the lowest level OU within the Active Directory tree that contains the user or account.

It is important to make note of this structure, because, by default, policy applied later overrides earlier policies. For example, a policy applied at the domain level would be overridden by a conflicting policy applied at the OU level. This precedence is true for policy settings set to Enabled or Disabled. Policies set to Not Configured are ignored and do not overwrite anything. Also note the exception to lower-level settings overriding higher-level settings: Computer policies will generally take precedence over user policies when there is a conflict.

This default inheritance behavior can be changed, however, as we will see next.

## Group Policy Inheritance

The default inheritance settings of Windows 2000 Group Policy can be changed via two settings:

- No Override
- Block Policy Inheritance

The following sections examine these settings.

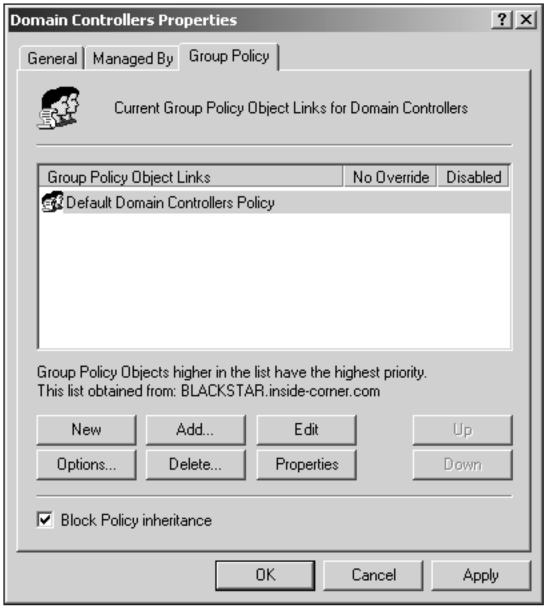
### No Override

No Override is set on a link, and not on a site, domain, OU, or specific GPO. In contrast, Block Policy Inheritance applies to a domain or OU, and therefore applies to all GPOs linked to that level or higher in the Active Directory tree. When in conflict, No Override will take precedence over Block Policy Inheritance.

No Override is used to prevent policies at lower levels in the Active Directory tree from overwriting policies applied at a higher level. For example, say you linked a GPO to a domain and set the GPO link to No Override, and then configured Group Policy settings within the GPO to apply to OUs within the domain. GPOs linked to OUs would not be able to override the domain-linked GPO.

### Block Policy Inheritance

Block Policy Inheritance will also prevent policies from higher in the Active Directory tree from being applied at lower levels of the tree. For example, if you had an OU policy and wanted to leave all settings unconfigured that weren't explicitly defined for that GPO, you would use Block Policy Inheritance to prevent a domain-level policy from applying settings to that OU. Block Policy Inheritance is enabled through a checkbox on the Group Policy tab of the specific domain or OU. Figure 10-6 shows an example.



Current Group Policy Object Links for Domain Controllers

| Group Policy Object Links | No Override | Disabled |
|---|---|---|
| Default Domain Controllers Policy | | |

Group Policy Objects higher in the list have the highest priority.
This list obtained from: BLACKSTAR.inside-corner.com

☑ Block Policy inheritance

**Figure 10-6** You can block policy inheritance of Group Policy settings at the specific domain or OU

To see GPO links, open the GPO in the Group Policy console, view the properties by right-clicking on the root node, and choose Properties. Click on the Links tab and click on Find Now after choosing the appropriate domain.

## Group Policy Processing

So far, you have learned that group policies are processed in the following order:

- Local
- Site
- Domain
- Organizational Unit

You have also learned that processing order can be affected through the No Override and Block Policy Inheritance options.The order of processing cannot be modified, even through No Override and Block Policy Inheritance, although the use of filtering can remove or block an individual part of the processing order, such as the OU.

Now that you know how Group Policy is processed in general, it is important to look at the processing of Group Policy as it applies to computer and user policies.

## Computer versus User Policy Processing

In addition to the processing order we just outlined, computer policies are processed before user policies. When the computer is booted up, the computer policy will process first. That processing will include any startup scripts that have been configured, as well as policy settings defined in the Computer Configuration container. Once computer policies have been applied, user policy begins. When a user logs on to the computer, any logon scripts that have been configured will execute. The logon scripts will be followed by policy settings configured for the User Configuration container.

## Synchronous versus Asynchronous Processing

So far, we have been discussing what is known as **synchronous** processing, which waits until one action is complete before beginning another. For example, computer policies are applied before the logon dialog box is displayed to the user, and then user policies are applied before the Explorer shell and desktop are presented to the user. This is the default behavior in Windows 2000.

The opposite behavior is **asynchronous** processing, which allows policies to process without waiting for the outcome of other policies. Computer and user policies will attempt to apply themselves at the same time, which can lead to undesirable side effects in many cases. Unless you have a specific reason to process Group Policy asynchronously, we recommend that you leave the default settings in place. Synchronous processing provides a higher degree of reliability.

## In Case of Conflict

In the event of conflict, a computer policy set in Computer Configuration will generally have precedence over a user policy set in User Configuration. In some cases, such as the Windows Installer policy Always Install With Elevated Privileges, the policy must be set on both the Computer Configuration and User Configuration nodes in order for it to be enabled.

## Periodic Policy Processing

Consider for a moment the following situation. You are the Group Policy administrator for 10,000 Windows 2000 systems on your corporate wide-area network (WAN). What happens if you modify a domain-linked GPO and you need to have it take place within a short period of time—say, two hours? Do you send out a global e-mail asking everyone to reboot? How do you handle the offices on the other side of the globe, where it might be the middle of the night and computers might be left on?

The answer lies with periodic refresh. System policies in Windows NT 4 can be changed only when a user reboots, at which point the new policy overwrites the old policy settings. But with Windows 2000, you can choose to have group policies processed periodically without requiring a reboot. The default settings process group policies every 90 minutes, with an offset of up to 30 minutes. An **offset** is a random amount of time applied to the 90-minute setting so that not every computer tries to process policy updates at the same time. If 5,000 computers all log on to the network at roughly 8:00 A.M. when work starts, you don't want all those machines hitting the servers simultaneously throughout the day to process Group Policy updates (even if no changes are made). The offset ensures that Group Policy requests are staggered, which eases the load on the servers.

In addition to the default setting of 90 minutes for workstations and servers, the default for domain controllers is 5 minutes. It is important not to specify too frequent a refresh policy in hopes of keeping the domain always up to date. Whenever a policy refresh occurs, the Windows shell refreshes as well. This action causes a momentary interruption in any user activity, which can range from annoying to intolerable depending on the refresh interval. It is best to balance carefully between regular policy refreshes and user inconvenience.

Exceptions to policy refreshes include:

- Software installation
- Folder redirection

For these two policies, periodic processing typically is not appropriate. For example, you wouldn't want a software installation to remove a particular application that might be in use. You also wouldn't change the location of folders when there might be open files from the old location.

In the event that you need to refresh Group Policy immediately, Windows 2000 offers a command-line Security Editor. The commands to refresh computer and user policies are

```
secedit /refreshpolicy MACHINE_POLICY
secedit /refreshpolicy USER_POLICY
```

These commands are useful when the refresh interval is set to a large amount of time and you need changes to take place right away.

Now that you have an understanding of the general concepts of Group Policy, it is time to look at some of the more concrete issues that you will face as an administrator of Group Policy. The first issue is possibly the most important: planning.

## GROUP POLICY PLANNING

As with most things in life, proper planning is the key to implementing a project successfully. Group Policy is no different in that regard. In this section, we will look at some of the design and planning issues you will face as you prepare to deploy Group Policy on your Windows 2000 network. These issues include:

- Change control procedures
- Structuring domains and OUs for Group Policy
- Segmented versus monolithic GPOs

- Cross-domain GPO links
- Managing network bandwidth
- Best practices

## Change Control Procedures

As you can probably already imagine, and as will become increasingly clear as we focus on specific policies, the effects of GPOs across a domain can be very complex. Therefore, one of the most important aspects of Group Policy administration is change control management.

With change control management, Group Policy administrators maintain records of all GPOs for an organization, including the following information:

- Name of the GPO
- Settings that the GPO applies
- Whether the settings apply to computers or users
- Specific sites, domains, and OUs to which the GPO applies
- Creation and modification dates
- List of specific changes that have been made since the GPO was created, and the names of the administrator(s) who implemented the changes
- Descriptions of changes and why they were made

Documentation is often tedious, and it is usually one of the first aspects of systems administration to be forgotten when your work queue is piling up with things that needed to be done yesterday. However, proper documentation will actually save you time in the long run, because you will be able to trace problems and procedures easily to their source. If you make a change to a GPO that doesn't take effect for several days, and you don't document the change, you may not realize at first the source of a problem that occurs because of the change. Even worse, in larger corporations with multiple administrators, much time can be wasted tracing problems if one administrator doesn't know about changes another administrator has made. With better efficiency, you'll spend less time in the fire-fighting mode in which systems administrators too often find themselves.

## Structuring Domains and OUs for Group Policy

Planning a domain and OU structure for Group Policy ties in very closely with your Active Directory planning in general—in fact, they go hand in hand. Two key issues face Group Policy planning:

- Delegation of permissions
- GPO location

Let's examine these issues in more detail.

## Delegation of Permissions

We will discuss delegating Group Policy administration a bit later in this chapter, but in this section we're referring to the delegation of administration for Active Directory in general. Whether you decide to administer Active Directory centrally or to distribute the administrative functions among a group of administrators in different locations will have an impact on how you should set up your domain and OU structure. For instance, if you are centrally managing your organization, you might want to have only a few GPOs implemented at the domain level. Note that a centrally managed infrastructure has a lot of flexibility at the OU level. Because you don't delegate administration of OUs, you have less restriction on how you place them in your organizational structure.

If your network spans multiple locations, however, and administrative functions are distributed among multiple administrators, it would make sense to look at a domain/OU structure that is more suited to that setup. If network administration is decentralized, permissions must be delegated to other Group Policy administrators. This setup can be less flexible, because the layout of administrative duties across the network may necessitate certain OUs existing in specific locations. The delegation of administrative responsibilities to multiple Group Policy administrators will play a role in determining the types of OUs you create and where you place them in the domain structure.

## GPO Location

Although we have touched briefly on the idea that the domain structure affects GPO placement, we haven't been very specific about the reasons. Consider a network that has 10,000 users in a single domain over four cities. The company has the standard collection of business units and a centralized MIS department that is responsible for all technology needs and services. The OU structure can take on any number of forms, depending on organizational needs. Each department can have its own OU, each physical location can be an OU, or even each city can be an OU, if some cities have multiple offices. Inherent flexibility is afforded to administrators of the centralized model because of the ability to assign OUs based on a variety of organizational models.

Now consider the same network—except that for political reasons, each physical location has its own administrator. In some cases, individual departments have their own administrators. This type of decentralized control suggests that certain OUs will exist in specific locations. For example, each location could have an OU, plus separate OUs can be created for specific departments required to maintain their own control. GPOs can be created that apply to the individual OUs, and administrative responsibility for them is delegated to local administrators. This scenario represents the decentralized approach to managing Group Policy.

Whether you choose centralized or decentralized management, it is important to design a structure that minimizes the amount of administrative overhead necessary to manage the network. Taking our previous examples, you can implement an OU structure in which you put all 10,000 users and computers in a single OU and assign permissions to that OU in such a way that local administrators control only the users and computers for which they are responsible. This is a terribly cumbersome approach. It's much better to create an OU for each administrator's area of responsibility and to give each administrator control over his or her particular OU.

This approach to OU structure applies to GPOs, as well. It makes more sense to create multiple smaller GPOs and delegate permissions to the GPOs rather than try to put the policy settings for the entire network into a few very large (monolithic) GPOs. This brings us to a point where we need to discuss the advantages and disadvantages of segmented versus monolithic GPOs.

## Segmented versus Monolithic GPOs

The type of OU structure that is implemented on your network may dictate whether to choose a segmented or a monolithic approach to designing GPOs. Centralized environments will tend to lean toward a monolithic design, whereas decentralized environments will lean toward a segmented design. Let's examine what these terms mean.

### Monolithic Design

A monolithic design uses a few very large GPOs, and is often implemented at the site or domain level. The GPOs apply to all users and computers on the network, regardless of OU membership. Group Policy processes more quickly because there are fewer objects to process. The downside is that delegation is difficult, because the few GPOs contain a large number of settings.

### Segmented Design

A segmented design is most often associated with decentralized administrative control, because that type of environment is more likely to have multiple administrators and delegated control over Group Policy. Segmenting GPOs creates smaller GPOs that contain fewer settings than those in a monolithic design. This design is much more flexible with respect to the delegation of administrative functions; however, performance is impacted because Group Policy takes longer to process an increased number of GPOs.

Quite possibly the best design for your organization will be a mix of monolithic and segmented GPOs. Keep in mind the advantages and disadvantages of each as you are planning your design, and use the appropriate type of GPO when implementing Group Policy.

## Cross-Domain GPO Links

With Group Policy, you must note a few considerations for networks that consist of multiple domains and possibly multiple sites. It is possible to create GPOs in one domain and have them apply to users and computers in another domain. However, doing so is not recommended in most cases, because computer startup and user logon are slowed—sometimes dramatically—if authentication must be processed by a domain controller from another domain. GPOs, you'll remember, reside within Active Directory. To apply a GPO, the target of the policy must be able to read the GPO. The overhead of additional authentication mechanisms to validate the computer or user account in the remote domain means that reading a GPO in a remote domain will not be as fast as reading a GPO in the same domain. Therefore, normally it is better to create duplicate GPOs in multiple domains rather than attempt to cross-link GPOs to other domains.

Other than the performance issue, there's no real reason not to cross-link domain GPOs rather than create multiple duplicate GPOs. In fact, a cross-linked single GPO is actually easier to manage—if you make a modification to the GPO, the change automatically applies to all users and computers in the sites and domains that link to the GPO. Otherwise, you will have to make the same change on every GPO that you created to perform the same functions in other domains.

Cross-domain GPO links work because the GPO links are contained in Active Directory, within the Global Catalog. All DCs in a forest share a single Global Catalog.

## Managing Network Bandwidth

Along the lines of domain-linked GPOs is managing site boundaries and network bandwidth. If your sites are set up correctly, you shouldn't have any problems; this area should be taken care of during the planning stages.

As with cross-domain linking, cross-site linking is possible because site objects are stored in the GC and replicated to all DCs in a domain. Because a site can span multiple domains, any GPO linked to a site will be replicated and applied to all computers and users within the site, regardless of domain or OU membership. Only the link information is replicated, though—not the entire GPO. Therefore, performance issues that apply to cross-domain linked GPOs will apply to cross-site linked GPOs, as well.

Proper site design holds that all subnets within a site are well connected—that is, connected by fast links. If a site does not follow those rules, however, and includes subnets connected by WAN links, then GPOs will be accessed across the WAN links and performance will suffer. Fortunately, Windows 2000 provides some built-in safeguards.

When Group Policy detects a slow link, rather than processing policy settings as normal, the following rules apply:

- Security Settings are always processed regardless of link speed.
- Administrative templates are always processed regardless of link speed.
- Folder Redirection is turned off.
- Software Installation is turned off.
- Internet Explorer maintenance is turned off.

Windows 2000 provides a policy template so that you can adjust these settings, with the exception that Security Settings and administrative templates cannot be disabled.

The default threshold for whether Windows 2000 considers a link to be slow or fast is 500Kbps. That speed is user configurable, however, so you can adjust the setting up or down, depending on your needs. A slow link can be either a WAN connection, such as a 384Kbps Frame Relay connection between sites, or a dial-up Remote Access Service (RAS) connection. Windows 2000 uses a complex formula to determine the current bandwidth, unlike Windows NT 4, which simply measures file-system performance. The formula for determining if a link is slow or fast for users and computers is as follows:

1. Using 0 bytes of data, ping the server and time the number of milliseconds. This value is time #1. If it is less than 10 milliseconds, then assume the connection is a fast link, and exit.
2. Using an uncompressible 2K of data, ping the server and time the number of milliseconds. This value is time #2. The algorithm uses a JPEG (.jpg) file that is already compressed. (If a compressible file was used, hardware compression on the adapter would compress it and make the network appear faster than it is.)
3. DELTA equals time #2 minus time #1. This value removes the overhead of session setup by assuming any time associated with time #1 is overhead (because it transferred 0 bytes). DELTA is the time in milliseconds to move 2K.
4. DELTA is measured three times, and the average of the three values is called AVG. Measuring three times provides a value that is more reliable and less susceptible to a temporary line condition that would skew the numbers.
5. The connection speed Z, measured in kilobits per second (Kbps), is figured as

   ```
   Z = 32000/AVG
   ```

The formula for this entire process is as follows:

```
(Z kilobits / second) = 2 * (2 kilobytes) * (8 bits/
byte) * (1000 milliseconds / second) / ( AVG milliseconds)
```

It sounds complicated, but the goal is to provide a reliable means of determining the real performance of the network connection.

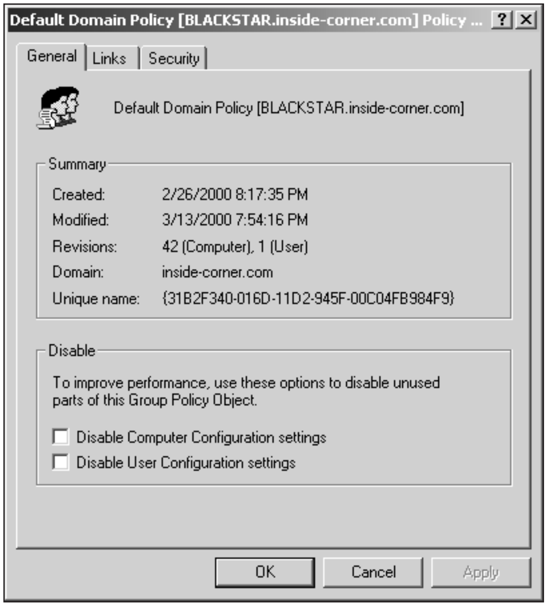
In addition to the speed settings for Group Policy, you can also set the speed that should be considered a slow or fast link for User Profiles. You configure this speed through Group Policy, in the Computer Configuration\Administrative Templates\System\Logon node. The user profile algorithm will attempt to ping the server first; however, if the client does not have support for the TCP/IP protocol, it will revert back to measuring the file system performance as in NT 4.

## Group Policy Best Practices

When planning your Group Policy implementation, there are some best practices to keep in mind. These are not hard-and-fast rules that you must follow, but rather they are some guidelines that could make your administrative life a lot easier. In this section, we'll give each tip its own heading with a description of why it is important.

## Disable Unused Portions of a GPO

As you browse through the Group Policy console, you can see that many settings are set to Not Configured. If you find that you do not need to use either the Computer Configuration or User Configuration portion of a GPO, you can disable one or both nodes to prevent Group Policy from processing it. For example, maybe you have created a GPO that applies specifically to user accounts in a domain. You are not using any of the computer policy settings in that particular GPO. By disabling the Computer Configuration node, you can speed up the processing of Group Policy, which won't process the node if it is disabled. Figure 10-7 shows the options to disable the computer or user policies; to reach this dialog box, right-click on the GPO root and choose Properties. If you decide to disable a node, you will receive the warning, shown in Figure 10-8, that asks you to confirm your choice.


Default Domain Policy [BLACKSTAR.inside-corner.com] Policy ...
?
General
Links
Security

Default Domain Policy [BLACKSTAR.inside-corner.com]

Summary

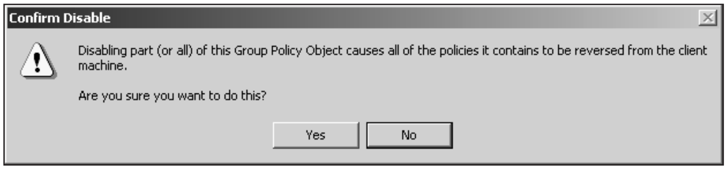
| | |
|---|---|
| Created: | 2/26/2000 8:17:35 PM |
| Modified: | 3/13/2000 7:54:16 PM |
| Revisions: | 42 (Computer), 1 (User) |
| Domain: | inside-corner.com |
| Unique name: | {31B2F340-016D-11D2-945F-00C04FB984F9} |

Disable

To improve performance, use these options to disable unused parts of this Group Policy Object.

□ Disable Computer Configuration settings
□ Disable User Configuration settings

**Figure 10-7** Disabling usused portions of a GPO can speed up Group Policy processing time



Disabling part (or all) of this Group Policy Object causes all of the policies it contains to be reversed from the client machine.

Are you sure you want to do this?

**Figure 10-8** Windows 2000 provides a stern warning about loss of settings before letting you disable a node

### Restrict the Number of Policies

It is important to note that the more policies you have applied to computers and users, the slower the logon startup process is. The guidelines are rather vague, and only through testing in your own environment will you know how many GPOs are too many. Faster machines and network connections can handle more policy settings in a shorter amount of time than slower machines or slower network connections. In general, be prudent with your policy decisions, and apply policies only where you specifically need to.

### Avoid No Override and Block Policy Inheritance When Possible

The No Override and Block Policy Inheritance settings can make it difficult to troubleshoot policy problems on a network, so it's best to avoid them when possible. They can also add a lot of complexity to your Group Policy setup. For example, suppose you block policy at a node, and then find that some areas need to have that policy overridden. Then, you put in some No Overrides to compensate. You quickly end up in a mess that is difficult to manage. This is not to say you should never use No Override and Block Policy Inheritance, only that you should use them cautiously.

### Use Group Policy Rather than System Policies

Windows 2000 corrects many of the shortcomings of NT 4's system policies, including the undesirable trait that system policies persist beyond their useful lives. Group Policy cleans up after itself whenever it refreshes (administrator configurable), and provides a wealth of new features.

### Filter Group Policy with Security Groups

As discussed in the next section of the chapter, "Group Policy Implementation," **filtering** is the process by which you allow or deny GPO access to individual computers or users or to groups of computers or users. As with general security management in Windows NT and Windows 2000, you should use security groups rather than apply policy settings directly to individual users and computers. It is much simpler to manage a single security group object than it is to configure dozens of user accounts individually, especially when modifications are made after the initial setup.

### Avoid Cross-Domain GPO Links when Possible

As previously discussed, creating cross-site and cross-domain GPO links has performance implications. If a slow link exists between domains or sites, the policy information will still have to pass over it during replication and user logons. Unless you have sufficient bandwidth, it is best to create duplicate GPOs in the other domains and sites.

### Limit the GPO Refresh Period

Having Group Policy settings refresh too often can put a serious damper on user productivity, because the Windows shell refreshes when the policy is updated. In most environments, policy settings are not constantly updated; so, choose a refresh interval that won't put too much of a burden on your computing environment.

Now that we have discussed the planning issues involved with Group Policy, it is time to shift our attention to the actual implementation.

# Group Policy Implementation

With concepts and planning under our belts, we turn to examining the implementation of Windows 2000 Group Policy. In this section we won't walk through all of the procedures, such as actually creating a GPO. Instead, in most cases we will simply describe the implementation details.

In this section, we will discuss the following topics:

- Creating a GPO
- Creating a GPO console
- Specifying Group Policy settings
- Filtering Group Policy
- Delegating administrative control of Group Policy
- Linking a GPO

## Creating a GPO

Before you do anything else with Group Policy, you must first create a GPO. In fact, without any GPOs created, you cannot even access the Group Policy Editor. Fortunately, Windows 2000 creates a GPO by default when you install Active Directory. It is the Default Domain Policy.

You create a GPO primarily through the Active Directory Users and Computers management console. From within the console, right-click on a domain or OU and select Properties. You will notice the options such as Add, New, Edit, and Delete. Those are the major commands, and they perform the following functions:

- *Add*—Add a Group Policy Object link
- *New*—Create a new GPO
- *Edit*—Modify an existing GPO
- *Delete*—Remove a GPO, a GPO link, or both

## Creating a GPO Console

In order to edit Group Policy settings, you must open the Group Policy Editor. The Group Policy Editor is the Graphical User Interface (GUI) for configuring GPOs; and, as you have learned, it provides the Computer Configuration and User Configuration nodes. You can open the Group Policy Editor in two primary ways: as a standalone tool or by editing a GPO.

Using the Group Policy Editor as a standalone tool, you can execute mmc.exe from a Run line and add the Group Policy snap-in. In Figure 10-9, we have opened a new blank console by executing mmc from a Run line. To begin the process of adding the Group Policy snap-in, choose Console|Add/Remove Snap-in.

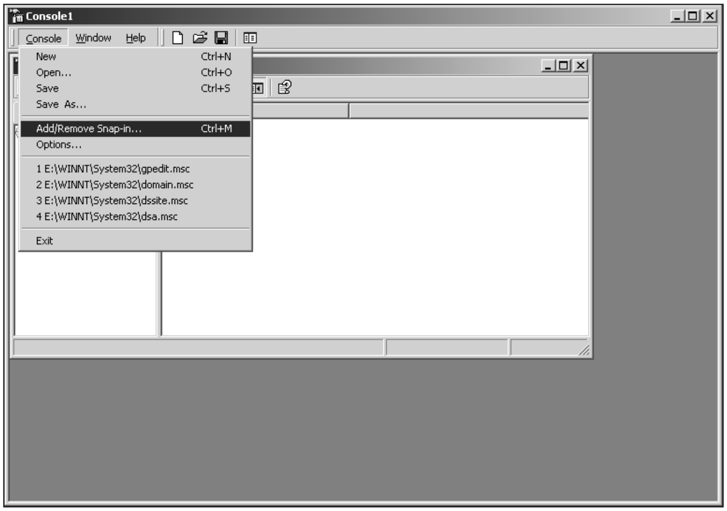
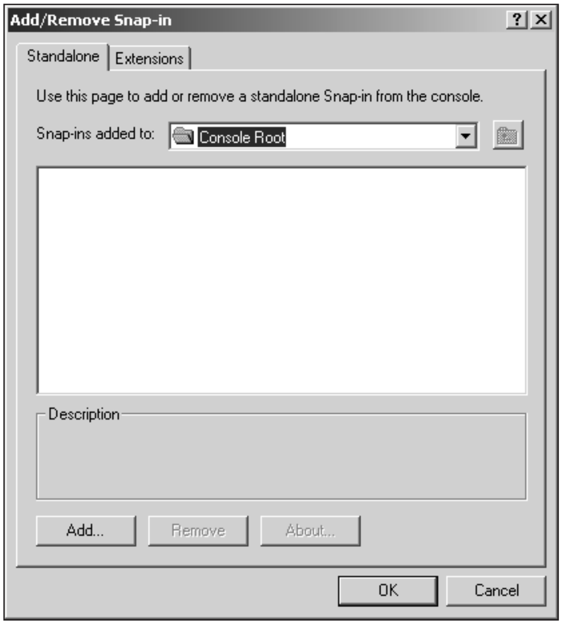

Console1
Console
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 E:\WINNT\System32\gpedit.msc
2 E:\WINNT\System32\domain.msc
3 E:\WINNT\System32\dssite.msc
4 E:\WINNT\System32\dsa.msc
Exit

**Figure 10-9** Click on Add/Remove Snap-in to get a list of standalone snap-ins to add to your console

Next you'll see the window displayed in Figure 10-10. It shows that currently you have not added any snap-ins to the console, and you have no available snap-ins to remove. Click on Add to add a snap-in.

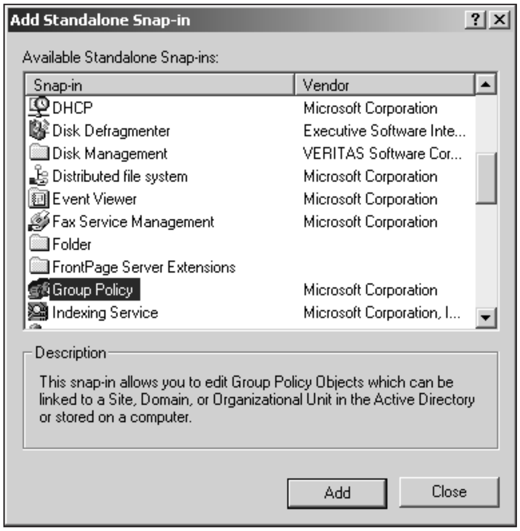


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

**Figure 10-10** In the Add/Remove Snap-in window, you can see a list of snap-ins currently associated with the console

When the Add Standalone Snap-in dialog is displayed, as in Figure 10-11, navigate to the snap-in for Group Policy. Highlight it and click on Add.

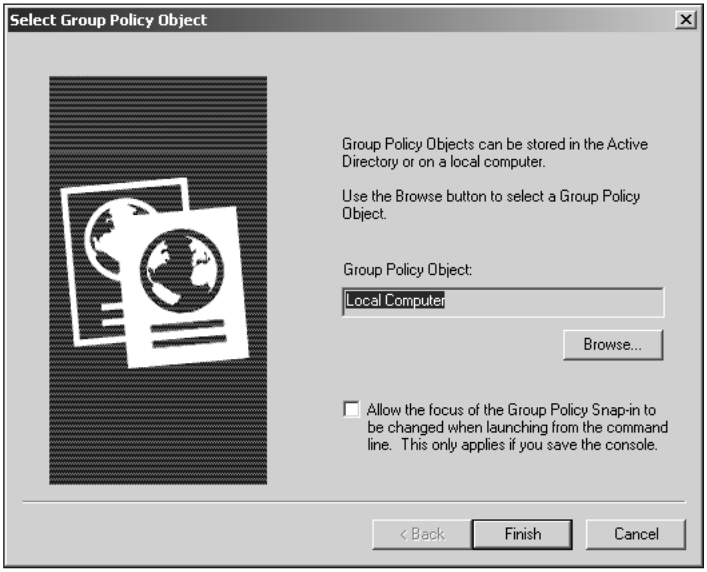


| Snap-in | Vendor |
|---|---|
| DHCP | Microsoft Corporation |
| Disk Defragmenter | Executive Software Inte... |
| Disk Management | VERITAS Software Cor... |
| Distributed file system | Microsoft Corporation |
| Event Viewer | Microsoft Corporation |
| Fax Service Management | Microsoft Corporation |
| Folder | |
| FrontPage Server Extensions | |
| Group Policy | Microsoft Corporation |
| Indexing Service | Microsoft Corporation, I... |

This snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

**Figure 10-11** You can select one or more standalone snap-ins to add to your blank console

Once you add the Group Policy snap-in, you are presented with the window shown in Figure 10-12. The snap-in will default to Local Computer. You can change it by clicking on Browse and choosing a different GPO for the focus, as shown in Figure 10-13.



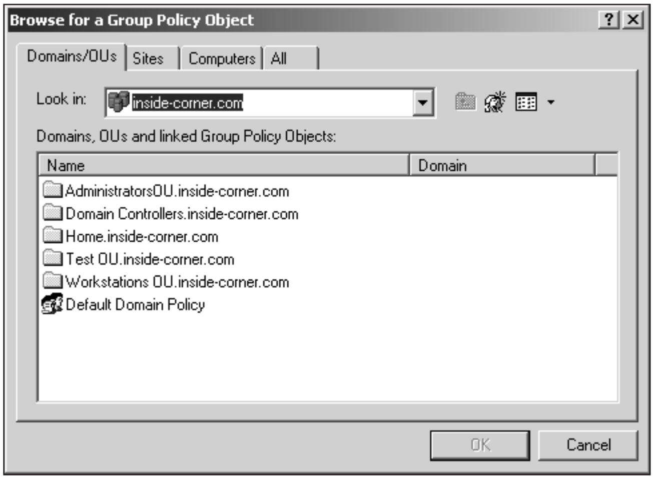
Group Policy Objects can be stored in the Active Directory or on a local computer.

Use the Browse button to select a Group Policy Object.

Group Policy Object: Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

**Figure 10-12** The Group Policy standalone snap-in defaults to the Local Computer for its focus



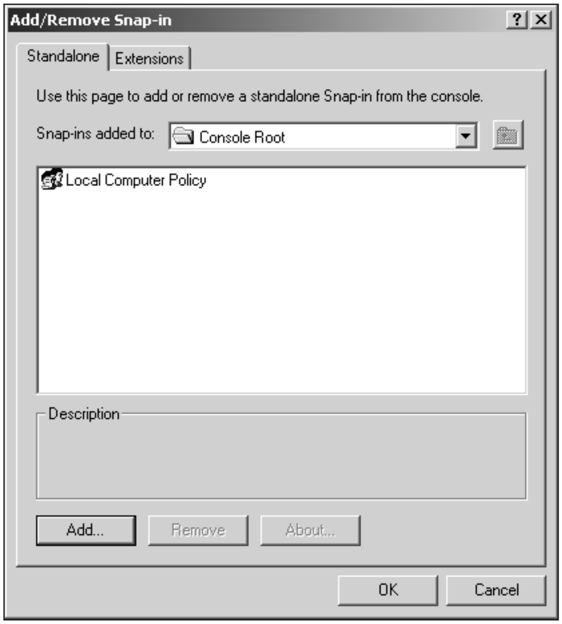
Look in: inside-corner.com

Domains, OUs and linked Group Policy Objects:

| Name | Domain |
|---|---|
| AdministratorsOU.inside-corner.com | |
| Domain Controllers.inside-corner.com | |
| Home.inside-corner.com | |
| Test OU.inside-corner.com | |
| Workstations OU.inside-corner.com | |
| Default Domain Policy | |

**Figure 10-13** You can change the focus of the Group Policy snap-in by choosing a different GPO from the available list

Once you've chosen your GPO, click on OK. You'll then see, as in Figure 10-14, that you have a snap-in to manage in the Add/Remove Snap-ins window. You can simply click on OK at this point to return to the console window and edit Group Policy settings.


Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Local Computer Policy

Figure 10-14 An entry now exists in the Add/Remove Snap-in dialog box

The other way to get a Group Policy Editor console with the focus on a GPO of choice is to go into the properties of a domain or OU in Active Directory Users and Computers and select the Group Policy tab. Editing a GPO from here will launch the Group Policy Editor.

Obviously, either of these methods is a tedious process to go through every time you want to edit Group Policy settings. The solution is to save your console by using the Console | Save As command. Give the console a descriptive name—like "Group Policy-*name of GPO*"—and OK it. Windows 2000 will save your custom console to the Administrative Tools folder, where you can access it easily in the future.

## Specifying Group Policy Settings

Once you have created your GPO and a GPO console, you're ready to edit the Group Policy settings. In Figure 10-15, we have created a Workstation OU to include all Windows 2000 Professional systems in our domain. The GPO name is reflected in the root node of the console.

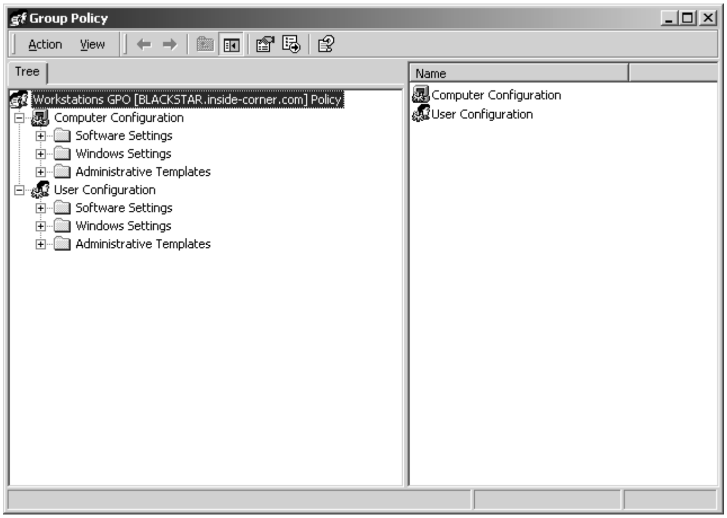


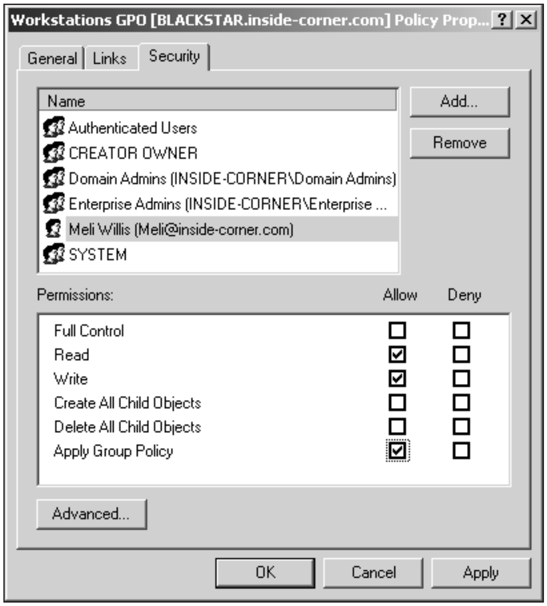
**Figure 10-15** With the Group Policy Editor focused on our new GPO, we're ready to start configuring settings

To configure settings, start expanding the nodes of the tree and exploring the settings you have available. Previously in the chapter, we discussed the Computer Configuration and User Configuration nodes and the subnodes beneath each of them: Software Settings, Windows Settings, and Administrative Templates.

## Filtering Group Policy

As we briefly mentioned earlier, Group Policy can apply only to users and computers that have Read permission for a Group Policy object. In fact, the easiest way to prevent certain users or OUs from receiving policy settings is simply to remove the Read permission to the GPO. This process is known as *filtering*, whereby you affect the groups of users and computers over which a GPO has influence. As discussed previously, a Group Policy object is the smallest unit in Group Policy; therefore, any filtering applies to the whole GPO. You cannot use security groups to filter only a portion of the settings in a GPO.

In order to filter GPOs through security groups, use the Security tab of a GPO's Property sheet. Figure 10-16 shows the Security tab for a Default Domain Policy GPO.


Workstations GPO [BLACKSTAR.inside-corner.com] Policy Prop...
General
Links
Security
Add...
Remove
Advanced...
OK
Cancel
Apply

Name

Authenticated Users
CREATOR OWNER
Domain Admins (INSIDE-CORNER\Domain Admins)
Enterprise Admins (INSIDE-CORNER\Enterprise ...
Meli Willis (Meli@inside-corner.com)
SYSTEM

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | ☐ | ☐ |
| Read | ☑ | ☐ |
| Write | ☑ | ☐ |
| Create All Child Objects | ☐ | ☐ |
| Delete All Child Objects | ☐ | ☐ |
| Apply Group Policy | ☑ | ☐ |

**Figure 10-16** You filter a GPO through the Security tab of a GPO's Property sheet

When filtering the effects of a GPO by security group, you are essentially editing the discretionary access control list (DACL) on that GPO. Using the DACL, you allow or deny access for users and computers to the GPO based on their memberships in security groups. In addition to DACLs, you also have access control entries (ACEs), which are the permission entries within a DACL. ACEs are permissions such as Full Control, Read, Write, and Apply Group Policy.

The Apply Group Policy permission, along with Read, allows users and computers to execute Group Policy settings. By default, all authenticated users have Read and Apply Group Policy permissions, but not Full Control or Write. This setup prevents ordinary users (non-administrators) from being able to modify GPOs. Microsoft recommends removing the Apply Group Policy permission from security groups that have had Read permission removed, because Group Policy will process more quickly if both settings are taken away. Apply Group Policy cannot function without Read permission to the GPO; keep that in mind as you are filtering Group Policy settings.

## Delegating Administrative Control of Group Policy

In decentralized environments, it is usually necessary to delegate some administrative control of Group Policy to other locations' administrators. Even in a large centralized environment, multiple administrators may be responsible for Group Policy administration.

Three Group Policy tasks can be delegated individually, as follows:

- Managing Group Policy links for a site, domain, or OU

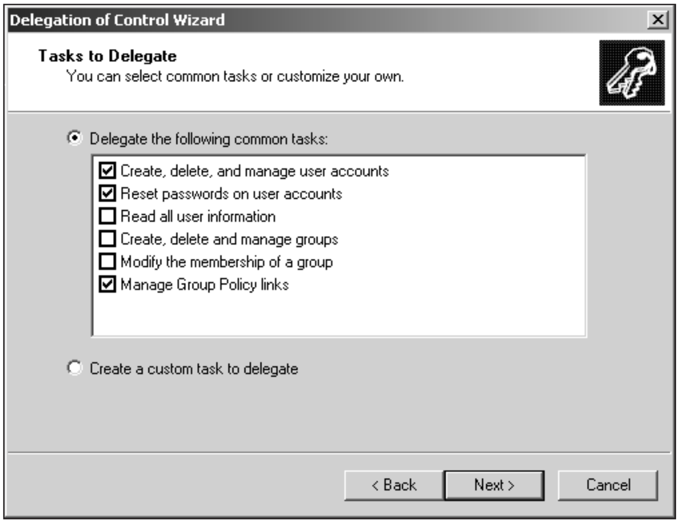
- Creating GPOs
- Editing GPOs

Local Group Policy applies to standalone computers only, whereas non-local Group Policy requires a Windows domain controller. The rights to administer Group Policy can be found under the <*GPO name*>\User Configuration\Administrative Templates\Windows Components\Microsoft Management Console node in the Group Policy Editor.

## Managing Group Policy Links

In order to delegate control to someone to manage GPO links, you must use the Delegation Of Control Wizard. To access this wizard, right-click on the domain or OU in Active Directory Users and Computers and select Delegate Control.

When the wizard starts, you are asked to select users or groups to which you want to delegate control. Once you have selected the appropriate personnel, click on Next. Then, you will see a window such as that in Figure 10-17, which shows a list of tasks to be delegated. Simply click on Finish after you have made your settings, and then click on Next; the wizard requires no other settings.



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

☑ Create, delete, and manage user accounts
☑ Reset passwords on user accounts
□ Read all user information
□ Create, delete and manage groups
□ Modify the membership of a group
☑ Manage Group Policy links

○ Create a custom task to delegate

**Figure 10-17** Windows 2000 allows you to choose the tasks you want to delegate using the Delegation Of Control Wizard

## Creating GPOs

You delegate the ability to create GPOs through Active Directory Users and Computers, as well. In order to create a GPO, a user account must belong to the Group Policy Creator Owners administrators group. Double-click on the Group Policy Creator

Owners group in the Users container, and click on the Members tab. Add the users who should be able to create GPOs.

### Editing GPOs

The ability to edit a GPO comes from being delegated administrative control of a specific GPO. To do this, open the GPO in the Group Policy Editor. Right-click on the GPO name and choose Properties, and then click on the Security tab. Add the user(s) you want to have administrative control and set the appropriate permission levels. At minimum, they will need Read/Write permissions, although you could go so far as to give Full Control.

## Linking a GPO

Before you can link a GPO, you must have at least the permissions listed previously to edit a GPO: Read/Write or Full Control.

To link a GPO, open Active Directory Users and Computers (or Active Directory Sites and Services, if you wish to link a GPO at the site level) and right-click on the domain or OU to which you want to link a GPO. Choose Properties, and then click on the Group Policy tab. Click on Add and navigate to select the GPO you want to link to the particular domain or OU. Click on OK when you are done. The GPO is now successfully linked to this domain or OU.

# Chapter Summary

Group Policy, as you have learned, is a powerful new feature of Windows 2000 for systems administrators. Its feature set far surpasses the system policies available in Windows NT 4, although Windows 2000 provides for backward compatibility with the older policies.

As we moved through the chapter, we discussed concepts of Group Policy such as:

- Windows 2000 Group Policy versus Windows NT 4 system policies
- Group Policy Objects (GPO)
- The Group Policy MMC snap-in
- Group Policy namespace
- Startup, shutdown, logon, and logoff
- Active Directory structure and Group Policy
- Group Policy inheritance
- Group Policy processing

In addition, we covered planning issues such as:

- Change control procedures

- Structuring domains and OUs for Group Policy
- Layered versus monolithic GPOs
- Cross-domain GPO links
- Managing network bandwidth
- Best practices

Finally, we finished up with a discussion of Group Policy implementation, covering the following topics:

- Creating a GPO
- Creating a GPO console
- Specifying Group Policy settings
- Filtering Group Policy
- Delegating administrative control of Group Policy
- Linking a GPO

Some of the key points to remember from this chapter include:

- GPOs can be applied at the site, domain, or OU level.
- Group Policy can help reduce TCO on networks, while increasing ROI for technology expenditures.
- Group Policy is processed in the following order: local, site, domain, Organizational Unit.
- The Group Policy Editor is the primary interface for modifying Group Policy settings.
- Policy settings can be blocked or overridden, if necessary.
- The use of Group Policy can impact the Active Directory domain and OU design process.
- Group Policy administration can be filtered or delegated.
- GPOs can be linked to other sites, domains, and OUs.
- When planning a Group Policy design, it is important to consider employee morale issues as well as technical issues.

In the next few chapters, we will expand on the knowledge of Group Policy that you've gained from this chapter, and explore managing the user environment with Group Policy, as well as deploying and managing with Group Policy. Windows NT 4 provides desktop management functionality through system policies, but it offers no equivalent for software management. And software management is a great new feature of Windows 2000.